REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. Rejections of Claims 18-32 Under 35 USC §102(e) and of Claim 33 Under 35 USC §103(a) in view of U.S. Patent No. 6,442,600 (Anderson)

In the Advisory Action dated July 21, 2004, the Examiner states:

> *It is true that Anderson does not teach preventing decryption of messages unless controls are implemented, however the claimed invention of claims 18-33 does not teach preventing decryption of messages unless controls are implemented.*

While the Applicant disagrees that the original claim 18 failed to "teach preventing decryption of messages unless controls are implemented," claim 18 has been amended to even more specifically recite that the system of the invention uses encryption to enable the viewer applet to control viewing and thereby implement sender controls on the message.

In contrast, the Anderson patent merely gives the recipient the option of having a message automatically deleted on the expiration date or of saving the message. The recipient is not prevented from doing anything that he or she wants to do with the message, and encryption is not involved in expiration of the message or in preventing the recipient from circumventing expiration controls by simply copying or saving the message and viewing it after the expiration date.

The purpose of the system of Anderson is to save **recipients** the trouble of storing, managing, and protecting received messages, as explained in col. 1, lines 20-29 and in particular in col. 1, lines 65 *et seq.* of the Anderson patent.

> *Some embodiments of the present invention provide a method and system for distributing electronic messages in an efficient manner using centralized storage and management. In particular, the system receives electronic messages to be distributed to one or more recipients, centrally stores a single copy of the message as well as various information about sending the message, and sends to each recipient a short indicator message to notify the recipient that the electronic*

> *message is available. The system then tracks and manages requests from the recipients to access the message by permitting access when appropriate, performing activities such as decrypting/encrypting the message if necessary, recording information about the access and about recipient instructions related to the message, archiving the message if necessary, and deleting the message when it is no longer needed. The recipient can also provide various instructions about actions to be taken with the message corresponding to an indicator, such as to save or delete the message or to forward the message to another recipient. In one embodiment, after all recipients have reviewed the message and no recipient has currently indicated to save the message (or all have indicated to delete the message), the system then deletes the single copy of the message).*

Nowhere does this passage disclose or suggest that tracking and management of messages is in response to controls selected by the originator or sender of the message **and implemented by means of encryption and a viewer applet on the recipient's computer**.

To implement the system of Anderson, there is no need for decryption to prevent viewing of a message except via a "viewer applet" that limits message access by the recipient. The only encryption provided for is encryption at the request of the recipient to limit viewing by third parties rather than the recipient. There are no limits on viewing of the message by the recipient, and any limitations that are selected by the message originator or sender are implemented by a message tracking table rather than a viewer applet, as claimed, that decrypts the message at the recipient's computer.

Because the Anderson does not disclose or suggest an electronic mail system that implements controls selected by the originator of the message rather than by an intended recipient, **using a viewer applet installed on the recipient's computer** to implement the originator-selected controls by preventing decryption of the message unless the controls (such as controls concerning expiration of a message) are implemented, it is respectfully submitted that the rejection of claims 18-32 based on 35 USC §102(e) in view of the Anderson patent is improper and should be withdrawn.

2. Rejections of Claims 1-17 and 34-50 Under 35 USC §103(a) in view of U.S. Patent No. 6,442,600 (Anderson) and U.S. Patent Publication No. 2003/1026215 (Udell)

This rejection is respectfully traversed on the grounds that the Udell publication, like the Anderson patent, fails to disclose or suggest the claimed viewer applet that enables reading of an e-mail message using the viewer applet, and yet that prevents viewing of the message, and **all incarnations** of the message after the expiration date of the message by ensuring that the message is only decrypted and viewed before the expiration date, or unless processing controls set by the message originator are implemented.

Instead of relying on a viewer applet installed on the recipient's computer (and encryption of the message to ensure that it can only be read using the viewer applet, the Udell teaches attachment of **executable code**, *i.e.*, a **virus**, to the message, which causes the user's system to destroy the message, while Anderson's system relies on software controlled entirely by the recipient to cause expiration. The virus of Udell is not used to ensure that it is the only means of viewing the message, but rather operates solely be destroying the message, irrespective of whether and how the message is viewed. Neither the Anderson patent nor the Udell patent discloses or suggests use of encryption to implement *sender* controls. **In the e-mail system of Udell, since a virus is used to destroy the message at the expiration date, there is no need for encryption to prevent viewing**. In the Anderson patent, expiration is **voluntary** on the part of the ***recipient***, and there is again no need to use encryption to prevent viewing of a message *by* the ***recipient***.

The claimed invention does not require the sender to attach any executable code to the message, but rather uses a viewer applet to enable reading of a message until the preset date sent by the user. **Each of the patents applied by the Examiner effectively causes message expiration, but neither does it in the claimed manner, by using encryption to prevent the recipient from a viewing a message in a manner contrary to the conditions set by the sender**. While encryption of messages is of course, encryption is used to prevent

third parties from a viewing a message. There is no suggestion in any of the references of record of using encryption to control how the intended recipient views a message.

Although the use of encryption to control how an intended recipient views a message is believed to be positively set forth in each of the original claims, the claims have nevertheless been amended to further emphasize this point. In particular, each of the claims now positively recite that the applet implements sender controls, and that since the message can only be viewed by using the applet, the applet ensures that controls, such as expiration of the message on a date or time set by the sender of the message, are positively implemented.

The recitation in claim 1 that the applet is used to decrypt and view the message only if controls set by the sender are implemented, clearly distinguishes the claimed applet from the virus of Udell. **Destroying a message at an expiration date, as taught in the Udell patent, is not the same as encrypting the message to control viewing as claimed**. In order to circumvent expiration of the message of Udell, it is simply necessary to disable the virus. If one disables the claimed "applet," one cannot view the message and therefore expiration of the message, or other controls, cannot be circumvented. The virus of Udell neither decrypts nor is used to view the message. It merely destroys the message.

In addition, neither the Anderson nor Udell patents suggests the use of a central server to **stream** messages to an expiration-date controlling viewer applet on the recipient's computer. As explained above, the Anderson patent discloses deletion of a saved message by a central "tracking table" associated with a "message distributor." Prevention of viewing is not carried out by a viewer applet on the recipient's computer. This is not only contrary to the claimed invention, but also fundamentally different than the approach taken by Udell, in which the central server that forwards e-mail plays no part in the message expiration and/or control, message expiration being controlled solely by a virus attached to the message. **According to the streaming method, the message is never present on the**

recipient's computer, and therefore there is no need to "destroy" the message as in Anderson or Udell.

Because neither the Anderson patent nor the Udell patent discloses or suggests control of message expiration by means of a viewer applet on the recipient's computer that provides access to the message prior to the expiration date through the use of decryption, and that prevents such access by ceasing decryption after the expiration date, withdrawal of the rejection under 35 USC §103(a) is respectfully requested.

Having thus overcome each of the rejections made in the Official Action, expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC

Date: August 23, 2004

By: BENJAMIN E. URCIA
Registration No. 33,805

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314
Telephone: (703) 683-0500